U.S. DEPARTMENT OF ENERGY

New Orleans, Louisiana
Monday, March 2, 2009 – Friday, March 6, 2009

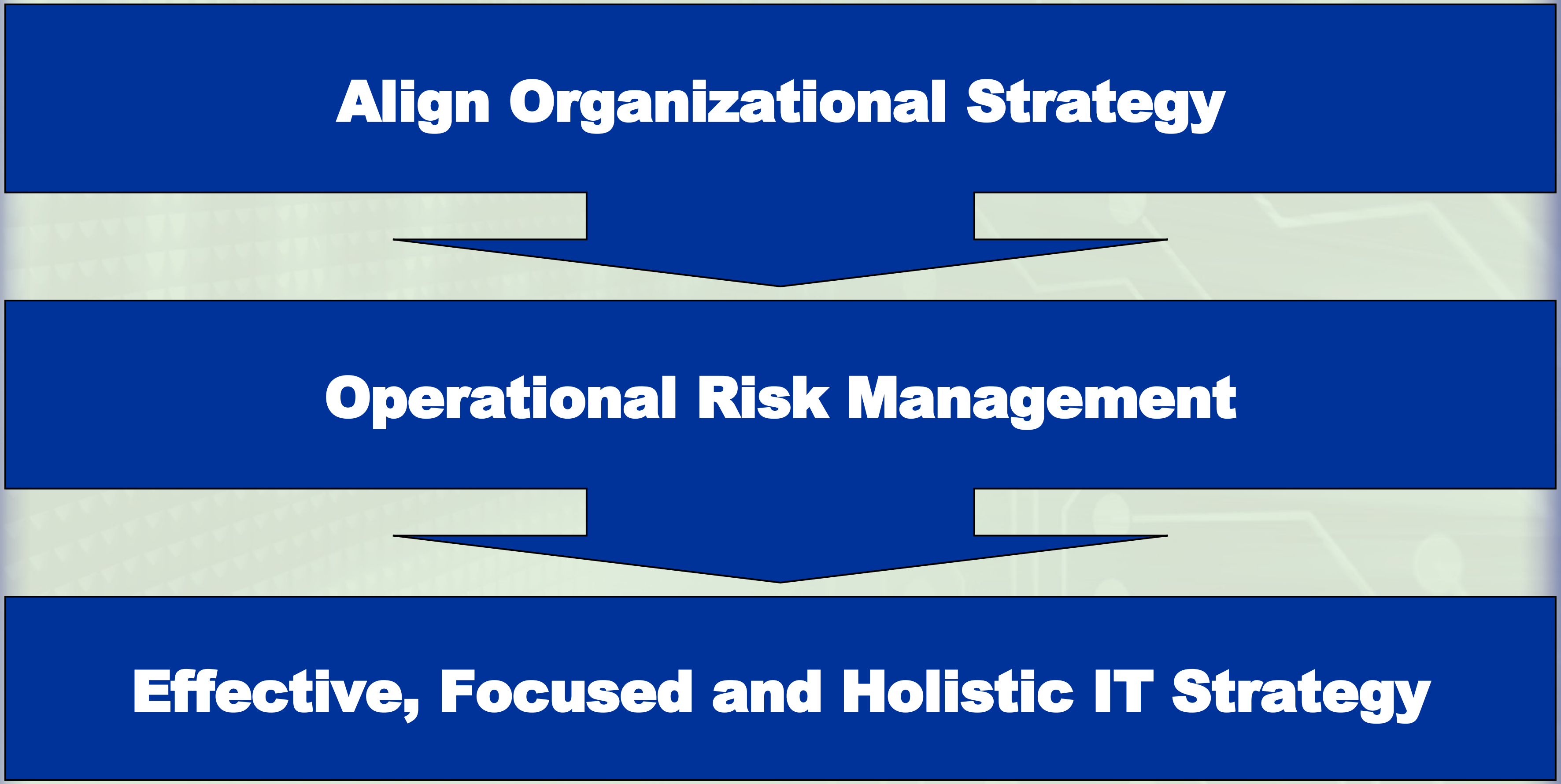
INFORMATION Management Conference

Raising the Bar...Seeking Innovative Solutions for Tomorrow's Challenges

Integrating Risk Management With IT Organizational Strategy

Phil Flewallen
VP, Strategy Management
1 Source Consulting

Today’s Focus



Align Organizational Strategy

Operational Risk Management

Effective, Focused and Holistic IT Strategy

Structured Approach to Organizational Strategy

- Many industry approaches are used for structuring Organizational Strategy.

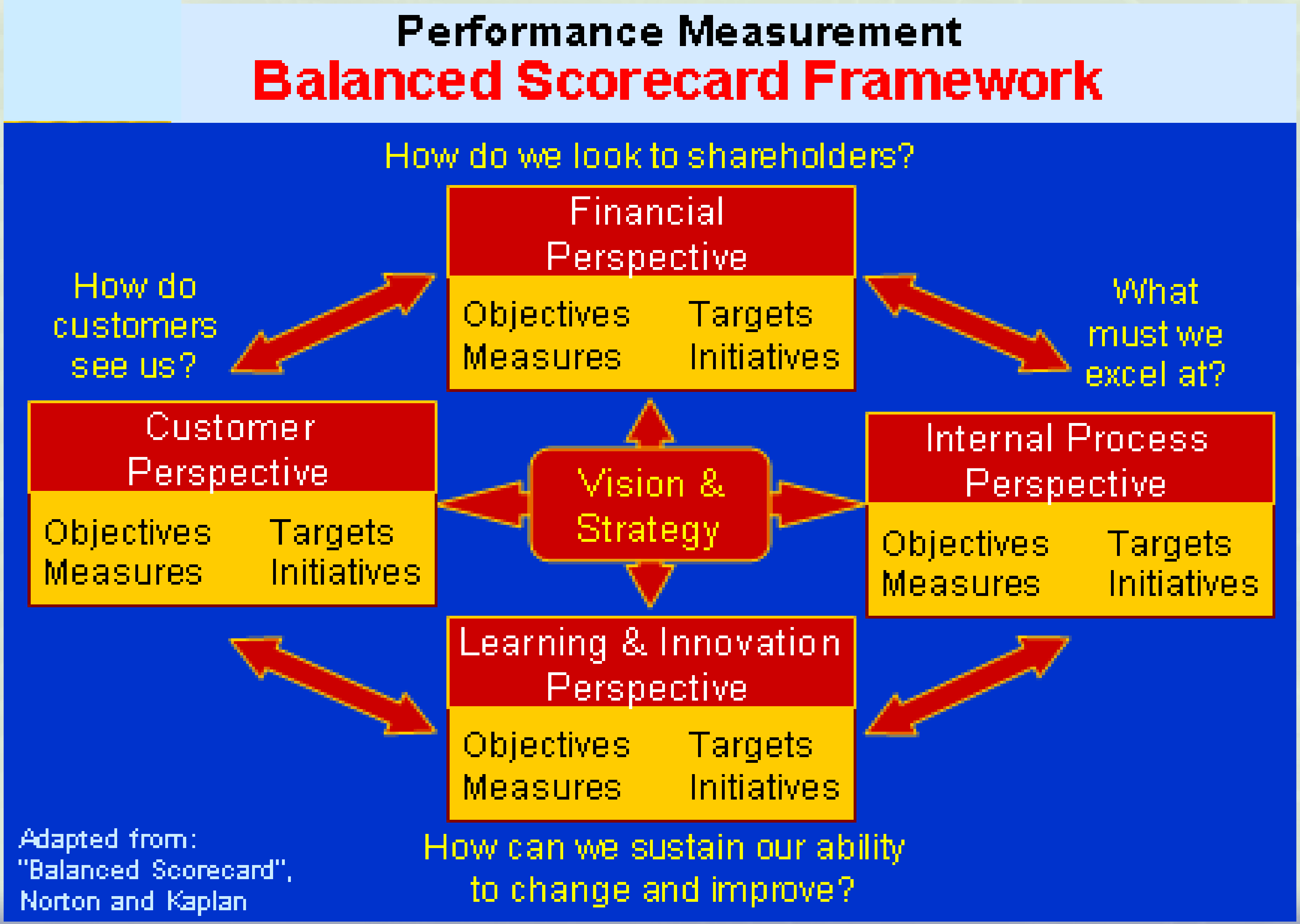
- Most methodologies do not include comprehensive risk assessment.

- The Balanced Scorecard is an integrating framework that can allow organizations a systematic way to manage risk in alignment with the organization’s strategy.

Balanced Scorecard (BSC) – *One Strategy, Multiple Views*

- Comprehensive
  - Encompasses the organizational mission, vision, core values, critical success factors, objectives, performance measures, targets and improvement actions.
- Communicated and translated into all business unit balanced scorecards
  - Division and team balanced scorecards
  - Performance plans of individual employees
- Applied to the IT function and its processes
  - A cascade of scorecards is instrumental in the IT/business governance processes
  - Hierarchy of scorecards supports the alignment of business and IT strategy.

Balanced Scorecard - Model



Performance Measurement

Balanced Scorecard Framework

How do we look to shareholders?

Financial Perspective

Objectives Targets
Measures Initiatives

How do customers see us?

What must we excel at?

Customer Perspective

Objectives Targets
Measures Initiatives

Vision & Strategy

Internal Process Perspective

Objectives Targets
Measures Initiatives

Learning & Innovation Perspective

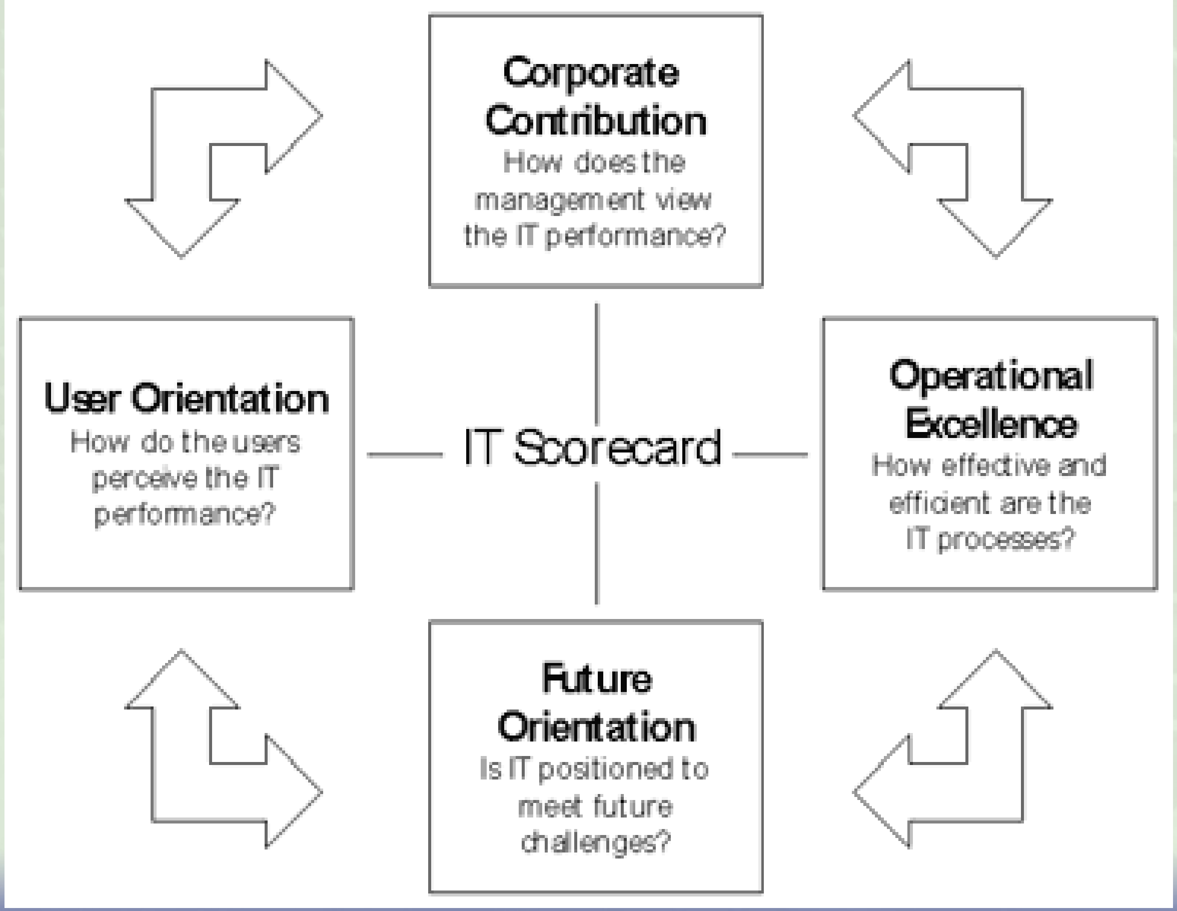
Objectives Targets
Measures Initiatives

How can we sustain our ability to change and improve?

Adapted from:
"Balanced Scorecard",
Norton and Kaplan

BSC IT Strategy - Best Practice Framework

- The following BSC IT Scorecard Framework enables alignment of the IT specific challenges in today's business environment.



Corporate Contribution
How does the management view the IT performance?

User Orientation
How do the users perceive the IT performance?

IT Scorecard

Operational Excellence
How effective and efficient are the IT processes?

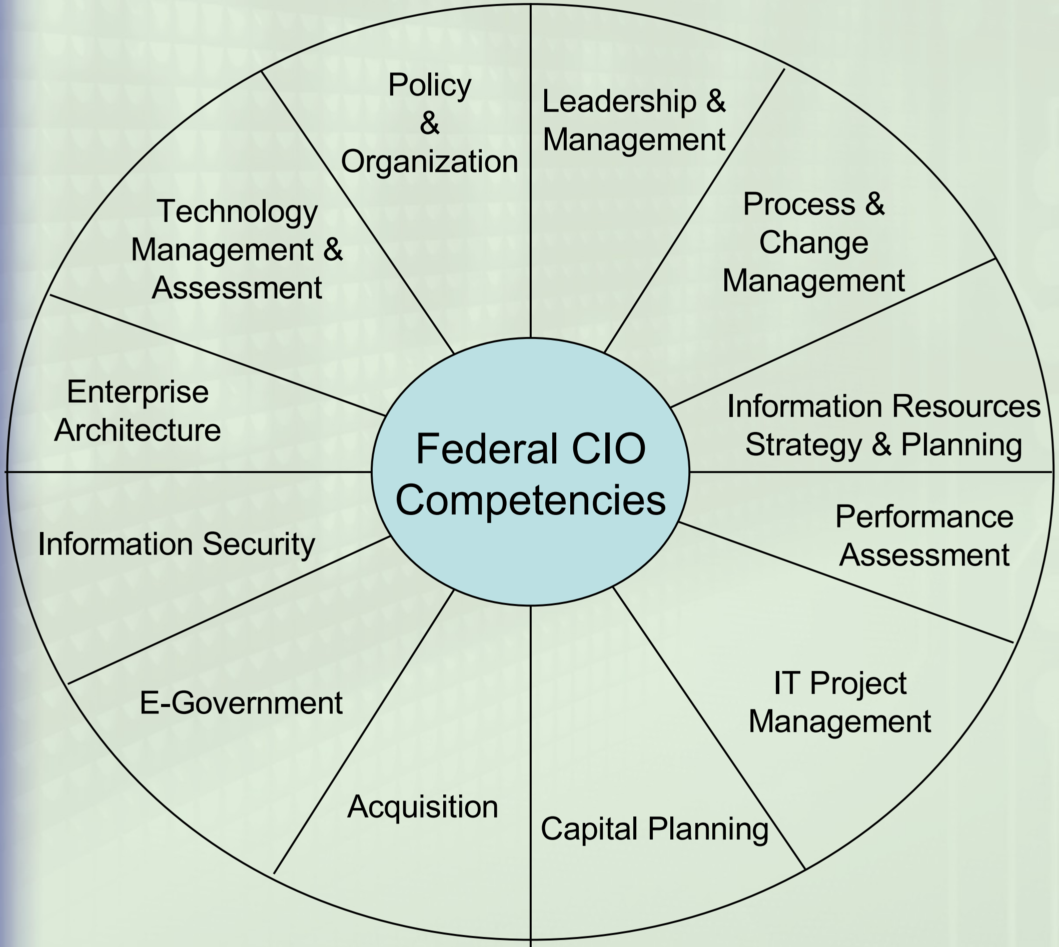
Future Orientation
Is IT positioned to meet future challenges?

BSC IT Strategy Framework

- Looking at the four perspectives of the IT scorecard we can start thinking about the content behind these perspectives, for instance:
  - **Corporate Contribution** – Obtaining a reasonable business contribution with IT investments, focusing on control of IT expenses, business value of new projects and business value of the IT function.
  - **User Orientation** – Becoming the preferred supplier of information systems and supporting business opportunities through IT, creating a real partnership and establishing a high level of user satisfaction.
  - **Operational Excellence** – Delivering efficient and effective IT products and services through efficient software development, hardware reliability and help desk support.
  - **Future Orientation** – Develop opportunities and answer future challenges, providing training and education, skilled IT resources, research and control of application portfolio aging.

Today's IT Roles

IT Leadership faced with broad range of responsibilities:



Potential risk is inherent within each area (from both a strategic and operational perspective)

Need to integrate risk management within the IT strategy is critical.

Properly identifying, measuring, managing, and reporting risk has become recognized as an extremely important initiative.

Clinger-Cohen – CIO Core Competencies

What is Operational Risk?

- Definition:
  - Risk of loss resulting from inadequate or failed internal processes, people or systems and from external events.
  - Includes:
    - Internal & External fraud
    - Employment Practices and Workplace Safety
    - Clients, Products & Business Practices
    - Damage to Physical Assets
    - Business disruption and system failures
    - Execution, Delivery & Process Management
    - Legal Compliance
    - Financial
- Technology risk management is a subset of Operational Risk.
- Operational risk management is a subset of a broader Enterprise Risk Management (ERM) program

What is Risk Management?

- Risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.
- In practical application, risk management is:
  - A process, ongoing and flowing through an entity
  - Impacted by people at every level of an organization
  - Applied in strategy setting
  - Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
  - Able to provide reasonable assurance to an entity's management and board of directors
  - Geared to achievement of objectives in one or more separate but overlapping categories

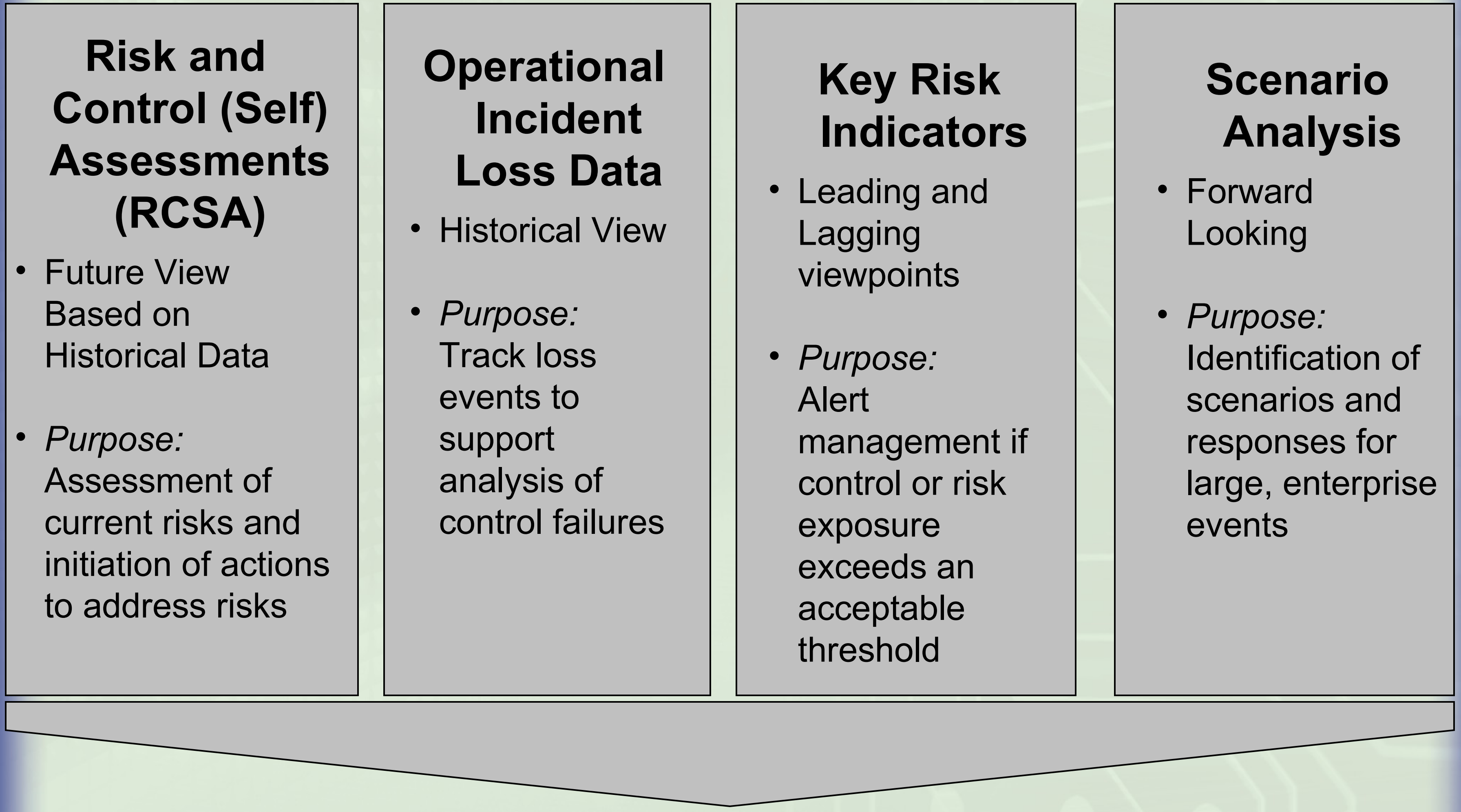
Value of Risk Management

- Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity’s objectives. Risk management encompasses:
  - *Aligning risk appetite and strategy*
  - *Enhancing risk response decisions*
  - *Reducing operational surprises and losses*
  - *Identifying and managing multiple and cross-enterprise risks*
  - *Seizing opportunities*
  - *Improving deployment of capital*
- These capabilities help management achieve the entity’s performance and profitability targets and prevent loss of resources.

Effective Management Requires a Solid Risk Framework

- Framework includes a taxonomy of the risks, controls, business processes.
    - Risks
        - *Hierarchy and definition of the risks the organization is interested in*
        - *Align with Business Drivers*
        - *Build off of industry standards, e.g., BASEL*
    - Controls
        - *Hierarchy of control types (e.g., access controls, data quality, etc.)*
        - *Build off of industry standards, e.g., COBIT*
    - Business Processes
        - *Consistent view of organization's business processes.*
        - *Must be in sync with business areas identified in Balanced Scorecard (or other Strategic Planning mechanism)*
- Framework also includes a defined methodology for Managing Risk
    - Procedures and standards for performing risk assessments, monitoring risk and reporting risk
    - Repeatable framework using standard risk scoring approaches
- Framework should be reviewed and updated annually to reflect lessons learned and current risk focus areas of the organization

Four Pillars to Unlocking Risk



Risk and Control (Self) Assessments (RCSA)

- Future View Based on Historical Data
- *Purpose:* Assessment of current risks and initiation of actions to address risks

Operational Incident Loss Data

- Historical View
- *Purpose:* Track loss events to support analysis of control failures

Key Risk Indicators

- Leading and Lagging viewpoints
- *Purpose:* Alert management if control or risk exposure exceeds an acceptable threshold

Scenario Analysis

- Forward Looking
- *Purpose:* Identification of scenarios and responses for large, enterprise events

Comprehensive View of Risk Position

Risk Control (Self) Assessments (RCSA)

- Goal:
  - Assess current operation and design of controls to minimize threats to the continuing efficiency, profitability, and success of operations.
- Risk Assessments include:
  - Identification and analysis of risks to which the organization is exposed
    - Likelihood/Frequency - probability of occurrence of events
    - Severity - value to the organization of consequences of events
  - Understanding of controls and their effectiveness to detect, prevent and/or mitigate risk
  - Determination to “accept risk” or implement actions to eliminate or reduce risk probability or severity.

Operational Incident Loss Data

- Goal:
  - Collect and assess control failures to identify control gaps, opportunities for improvement and gauge effectiveness of control environment
- Operational Incident Programs include:
  - Awareness and training to encourage reporting
  - Structured program to assess events
  - Standards of reporting (who, when, escalation thresholds, etc.)

Key Risk Indicators

- Goal:
  - Monitor detective and preventive risk indicators to alert teams to potential control failures
- KRI Programs include:
  - Develop detective and preventive risk indicators
  - Develop a risk dashboard for different audiences
  - Transition to automated alerts and real-time monitoring

Scenario Analysis

- Goal:
  - Discuss worst case scenarios to understand potential and current control responses
- Scenario Analysis Programs include:
  - Targeted scenarios for low frequency, high impact events, e.g. terrorist strike
  - Cross-divisional participation

Where does IT Risk Fit Within the Organization?

- Many organizations already integrate IT into their organization-wide risk management initiatives.
- However, others are evolving. IT risk functions may be:
  - Separate
  - Component
  - Integrated

Organizational Evolution of IT Risk

1. **Separate Functions**

- When IT and the business are not aligned, IT and operational risk have an arm's length or nonexistent relationship.
- IT risk is often focused on security and compliance issues, with little input or interaction with business decision-makers or operational risk managers.
- Though different factors may spark the change, today previously separate risk organizations are beginning to develop formal relationships.

Organizational Evolution of IT Risk

2. Component Functions

- Under this model, IT risk is considered a section of an organization’s overall risk strategy.
- Enterprise Risk Management (ERM) serves as the risk umbrella, and IT risks are represented in the overall risk picture.
- While IT risk should be part of a portfolio of risks, there is value in granting special attention and resources to IT risk.
- IT risk is then reported along with other enterprise risks through a layer of committees as part of the organization’s aggregate risk picture.

Organizational Evolution of IT Risk

3. **Integrated**
   - As the relationship between IT risk and ERM evolves, the two risk domains become more integrated in both process and organizational structure.
   - Progresses from reporting metrics to providing input on risk management processes and strategy.
   - IT’s risk managers should sit on committees with their ERM counterparts to formulate macro-risk strategy,
   - ERM becomes incorporated into IT’s disaster recovery/business continuity steering committees and other IT risk activities.
   - Benefits
     - Greater understanding between IT and the business
     - Higher visibility of risk from the business side
     - Aligned risk management strategies
     - More comprehensive risk assessments and audits.

Understanding Business Change And IT Risk - Best Practices

- **Risk Management should be integrated with Business Decisions:**
  - Business Change Initiatives - Engage risk management teams to assess underlying risks of change, including control structures, infrastructure needs, etc.
  - Product/Solution Acquisitions - IT and the business work together to evaluate and quantify the risks associated with a new acquisition before procurement completion.

- **Shift IT into a proactive role:**
  - IT can help shape the business decisions by examining emerging technologies from a risk perspective.
  - IT can assist the business in spotting opportunities and understanding the associated risks before a project or change is even conceived.
  - IT becomes more strategic and can help shape changes to avoid risk.

The IT Organization today:

- **Struggles with Matching Business Pace**
  - As the business adapts to remain competitive, managers of IT organizations worry that they will not be able to upgrade complex infrastructure or replace legacy applications quickly enough to support business needs.
    - The mismatch between business pace and IT support further erodes business perception of IT and makes it difficult to get the business to accept IT in a strategic, nontechnical role.

The IT Organization today:

- **<u>Focuses on compliance</u>**
  - The proliferation of regulatory guidelines makes compliance an urgent business priority.
  - The needed focus and funding for compliance threatens to create IT tunnel vision, so managers are not seeing other critical domains of risk.
  - IT and information security departments are concentrating on changing policies and procedures to fit within the “letter of the law.”
  - There is a further disconnect as compliance is tackled as siloed projects that fail to be integrated into broader risk and control processes.

The IT Organization today:

- **Worries about security**
  - CIOs and managers consistently identify IT security as one of their top risks.
  - The recent wave of high-profile security breaches illustrates the importance of strong security controls.
  - Challenge - IT's increased accountability in this area has caused many organizations to falsely equate IT risk with security and related compliance issues, leaving it vulnerable in other areas.

Not Just Information Security Risk…..

- IT organizations typically define risk in terms of security and compliance.
- However, risk encompasses much more than security
- Narrow attention to one component of risk leaves the organization unprepared and unprotected in other important areas.
- To transition to a more holistic approach, IT needs to become better aligned with the business.
- Let’s look at 4 Categories of IT Risk
  1. Business Disruption Risks
  2. Relational Risks
  3. Technology Risks
  4. IT Governance Risks

IT Risk Domains
- Business Disruption Risks

Business disruption risks include malicious attacks and online privacy issues, as well as external events that could hinder a firm's continued operations.

- *Business continuity risk*
- *IT security risk*
- *Online risk*
- *Information risk*

IT Risk Domains
- Relational Risks

Relational risks emerge from dependency on third parties and the business' perception of IT as shaped by the frequency of service disruption and the effectiveness of IT's communications

- *Vendor management risk (suppliers)*
- *Third-party relationship risk with partners (outsourced relationships)*
- *IT reputation/customer satisfaction risk*

IT Risk Domains
- **Technology Risks**

Ability to keep pace with new technology, manage and develop projects that address business needs, implement business changes in a responsible manner, and maintain a standardized but flexible IT infrastructure.

- *IT agility risk*
- *IT architecture risk*
- *Change execution risk*
- *Project development risk*

IT Risk Domains
- IT Governance Risks

Universally recognized as an important risk for businesses regardless of industry. Without a strong governance structure in place, organizations will be unable to mitigate the IT risks associated with other domains.

- *IT strategic risk*
- *IT resources risk*
- *Compliance/legal risk*

INFORMATION Management Conference

Summary

- To implement a successful IT risk program, organizations must:
  - Address all aspects of IT Risk
  - Align with and support the organization’s business strategy.
  - Ensure IT Risk Management looks at the needs of the organization, aligning business concerns with IT concerns
  - Define and execute an overarching and ongoing strategy to address all critical risk factors

INFORMATION Management Conference

Discussion - Questions